UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/810,731	03/16/2001	Curtis E. Stevens	00-1015	6847

42645 7590 11/01/2005

PHOENIX TECHNOLOGIES LTD.
915 MURPHY RANCH ROAD
MILPITAS, CA 95035

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 11/01/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/810,731	STEVENS, CURTIS E.	
	Examiner	Art Unit	
	Thanhnga B. Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08/08/2005 (Amendment)*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 March 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's amendment filed on August 8, 2005 has been entered. Claims 1-18 are pending. Claims 1-2, 6-8, 12-14, and 18 are also amended by the applicant.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moos (US 5,881,152), and further in view of Kramer et al (US 5,414,852) and further in view of Shpuntov et al (US 5,917,928).

a. *Referring to claim 1:*

i. Moos teaches:

(1) causing a calling process desiring to gain access to the protected area to locate an interface that permits access to the protected area **[i.e., the programmable processor manages such a linkage of information stored on the diskette and the physical data storage medium with the ID of an authorized user or process with access to this information. The ID of the user or process is checked by the intelligent processor chip via a separate interface. If the ID of the authorized user or process cannot be proven to the processor chip, access to the stored information is denied (column 3, lines 24-31)]**;

(2) causing the calling process to use the interface to create a trusted relationship between the calling process and system firmware **[i.e., the contents of a data storage device are linked to the personalized key from an active storage device using a cryptographic process and are, thus, sealed. Any changes made by "third parties" can thus be detected at any time, since only "known" systems are capable of generating valid data storage media, securing data integrity, and establishing the singularity of the data through a reference.**

System components or users are defined as "known" by being recognized by all system components or users involved in the system (column 35-43)];

(3) once the trusted relationship has been established, allowing the calling process access to retrieve a directory of service areas in the protected area **[i.e., copying of the stored information can be prevented or verified using information generated and managed by the processor and stored on the data storage device (column 3, lines 32-34)];**

ii. Although Moos does not clearly and explicitly point out :

(1) allowing access to one or more service areas in the protected area; processing data contained in the one or more service areas; and closing the protected area when processing data in the one or more service areas is complete **[i.e., Moos implies: the ID of the user or process is checked by the intelligent processor chip via a separate interface. If the ID of the authorized user or process cannot be proven to the processor chip, access to the stored information is denied, which means that if the ID matches the data in the target system, the authorized user allows to access to the stored information (column 3, lines 27-31)].**

iii. In addition, Kramer teaches:

(1) Permission to perform only selected functions on data is also common. For example, users may be given access to selected files for only limited purposes. Users may be allowed to only read the particular data file, they may be allowed to read from a file and write (update) that file, or they may be authorized to read, write and delete that file. Access lists can be used to designate which users have some or all types of access to any particular file or groups of files **(column 1, lines 18-26).** Furthermore, if permissions are used, it is possible to provide a default user access symbol having restricted permissions, such as read only. In this case, the access list would have an individual list of users which need write and delete privileges, while the default symbol, which selects any other users, has only read permission. A similar technique can be used for the data managers, in a situation in which access is to

be restricted only by user identifier, with any data manager having access to the object **(column 5, lines 59-67 of Kramer).**

iv. Although Moos and Kramer do not clearly mention the closing process, Shpuntov teaches:

(1) Referring to Figure 2, the control unit 12 then ends the enrollment control program at step 144 **(column 10, lines 6-8 of Shpuntov).**

v. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) clearly point out the entire process of accessing the stored information in the protected area of the storage device for protecting stored data, and more particularly for preventing or identifying tampering of stored data **(column 1, lines 6-8 of Moos).**

vi. The ordinary skilled person would have been motivated to:

(1) clearly point out the entire process of accessing the stored information in the protected area of the storage device since access to such information can be protected, for example, by cryptographic methods which encode the data. However, the encoded information can still be physically copied in a simple manner. In the case of such information stored on data storage media for archiving or transmission, the possibility exists in general that the information can be manipulated by unauthorized third parties before it is further processes **(column 15-23 of Moos).**

b. *Referring to claim 2:*

i. Moos further teaches:

(1) sending a public key to the system firmware; modifying the public key using a private key using the system firmware; causing the calling process to validate the modified key; causing the system firmware to issues a public key to the calling process; modifying the public key using the private key using the calling process; causing the system firmware to validate the new key; and if the key is not validated, granting not access to the protected area; and if the key is validated, granting access to the protected area **[i.e., referring to Figure 3, a standard algorithm generates a unique compressed form of the data, as shown in step 102**

of FIG. 3. This compressed data is provided with an ID (step 104) and a signature count from the chip. The data is encrypted with the secret part of the asymmetric key (step 106), and is stored in the memory area of the chip (step 108). The signature counter status is entered into the data storage medium to be protected. The functionality of the secret asymmetric key is secured with the help of a so-called "challenge and response" with the aid of the symmetric key. This means that the user group-dependent symmetric key must also be contained in the security software. An authorized target system can uniquely identify a data storage device thus secured. For this purpose, a challenge and response exchange is carried out between the software and the chip and thus the validity of the data storage device is established. Subsequently the data is read in the conventional manner and compressed with the same algorithm used for writing. The cryptogram obtained after writing to the data storage device is read from the memory of the chip and decoded using the public part of the asymmetric key (column 2, lines 61-67 through column 3, lines 1-14)].

c. *Referring to claim 3:*

i. Moos/Kramer further teaches:

(1) returning a handle from the system firmware to the calling process once the system firmware has learned to trust the calling process; modifying the handle using the calling process; returning the modified handle to the system firmware as a part of the retrieve directory request; and allowing the calling process to locate the desired service area using the information returned by the retrieve directory request **[i.e., these limitations are taught by the Moos/Kramer combination (see claim 1 rejection and Figure 1, column 2, lines 25-67 through column 3, lines 1-34)].**

d. *Referring to claims 4-5, 9-11, 15-17:*

i. These claims have limitations that is similar to those of claim 3, thus they are rejected with the same rationale applied against claim 3 above.

e. *Referring to claims 6-7, 12-13, 18:*

i. These claims have limitations that is similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above.

f. *Referring to claims 8, 14:*

i. These claims have limitations that are similar to those of claim 2, thus they are rejected with the same rationale applied against claim 2 above.

Response to Argument

4. Applicant's arguments filed August 8, 2005 have been fully considered but they are not persuasive.

Applicant argues that:

Some limitations such as "once the trusted relationship has been established, allowing the calling process access to retrieve a directory of service areas in the protected area, and allowing access to one or more service areas in the protected area" which are not taught or suggested by the combination of references as cited by the Examiner.

Examiner totally disagrees with the applicant and still strongly maintains that:

The combination of teachings between Moos, Kramer and Shpuntov do teach the claimed subject matter. In fact, Moos further teaches the programmable processor manages such a linkage of information stored on the diskette and the physical data storage medium with the ID of an authorized user or process with access to this information. The ID of the user or process is checked by the intelligent processor chip via a separate interface. If the ID of the authorized user or process cannot be proven to the processor chip, access to the stored information is denied (column 3, lines 23-30 of Moos). In addition, Kramer clearly teaches the same subject matter for protecting data in a computer system. Furthermore, Kramer discloses a data processing system include a plurality of data objects which are accessible by application programs through a system level interface. Each data object has an associated user access list. In addition, each object has at least one key indicating which applications can access that object. The key is preferably maintained in a protected storage area, accessible only by the low level system interface. Both the application identifier key and

the user who invoked that application must match the identifier information in the data object for access to be allowed to that object. If an unauthorized user attempts access to the data object through the correct application, or an authorized user attempts access through an incorrect application, access to the data object will be denied by the low level interface (see Kramer's abstract). Besides, referring to Figure 4 of Kramer, the decision making process performed by the system level interface 20 is shown in the flow chart of FIG. 4. When a call is made to the system level interface to access an object, the data object is identified 60 and the type of access which has been requested is identified 62. A check is made to determine whether the user responsible for the request is on the access list for that data object 64, and if not access to the data object is denied 66. If the user is on the access list, control is passed to block 68 in which a check is made to determine whether a user has permission for this type of access. If not, access is again denied 66. If the user does have permission for this type of access, a determination is made 70 whether all of the requesting list of data managers are in the key list for the object. If not, access is denied 66. If the data managers are on the key list, the system determines 72 whether they have permission for this type of access. If not, access is denied. Only if all possible elements are correctly matched is access granted 74 (column 5, lines 23-41 of Kramer).

Therefore, in response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the combination of teachings between Moos, Kramer and Shpuntov are clearly sufficient.

Moreover, Moos, Kramer and Shpuntov do not need to disclose anything over and above the invention as claimed in order to render it unpatentable or anticipate. A recitation of the intended use of the claimed invention must result in a structural

difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claimed limitations.

For the above reasons, it is believed that the rejections should be sustained.

Conclusion

5. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

a. Ooe (US 5,901,328) discloses a system for transferring data between main computer multiport memory and external device in parallel system utilizing memory protection scheme and changing memory protection area.

b. Arnold (US 6,175,924 B1) discloses a method and apparatus for protecting application data in secure storage areas.

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

TBT
October 20, 2005

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100